International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN (P): 2249-6831; ISSN (E): 2249-7943
Vol. 7, Issue 4, Aug 2017, 25-30

SECURE AND FASTER KEY MANAGEMENT OF ELLIPTICAL CURVE CRYPTOGRAPHY IN VANETS

EKTA NARWAL & SUMEET GILL

Assistant Professor (Computer Science), Department of Mathematics, M.D. University, Rohtak, India

ABSTRACT

Vehicular ad hoc networks (VANETs) use many types of cryptographic approaches for the security of messages during communication. Elliptical Curve Cryptography (ECC) is one of them and best among all other techniques, because the keys produced using elliptical curves are smaller in size. All keys are stored in Temper Proof Devices (TPDs) for security reasons. But, these devices are the first target for attackers to get the keys. Hence, researchers are trying their best for improving the cryptographic approaches. In this paper, we will try to secure the keys used in ECC from intruders and hence make them more secure

KEYWORDS: Vehicular ad hoc Networks (VANETs), Wireless Ad Hoc Networks (WANETs), Elliptical Curve Cryptography (ECC),Data Security & Artificial Neural Network (ANN)

Received: Jun 21, 2017; **Accepted**: Jul 08, 2017; **Published**: Jul 12, 2017; **Paper Id:** IJCSEITRAUG20174

Original Article

INTRODUCTION

Wireless ad hoc networks (WANETs) are decentralized wireless networks, which do not have any pre-existing infrastructure like wired networks, due to routers and access points [1]. WANETs can be further classified into two categories mobile ad hoc networks (MANETs) and Vehicular Ad Hoc Networks (VANETs). MANETs develop the connection between various mobile devices whereas VANETs are used to connect vehicles and roadside units. VANETs are becoming popular because, they provide vehicle to vehicle, vehicle to infrastructure and infrastructure to vehicle communication. These approaches are best for road safety, traffic management, toll payment, broadcasting informative messages for security alerts, weather forecasting messages. These include safety of driver's personal information, bank details, security of messages containing private information, security of keys stored in the intelligent vehicle, security of identity and many other issues [2]. Many cryptographic techniques are used for security in VANETs; ECC is one of the newest branches of security based on the arithmetic of the elliptical curves [3]. It comes under public key cryptography mechanism which provides encoding, digital signatures, key exchange and decoding. ECC provides better security with small size security keys in comparison to other cryptographic techniques. It also provides faster computations, low power consumption, less memory storage and saves bandwidth. All the security keys are stored in the hardware modules like tamper proof devices or temper resistance devices present in intelligent vehicles [4]. But, these devices are not secure from intruders. So, in this paper, we are focusing on a new approach by using Neural Networks for securing the private keys/ security keys used in elliptical curve cryptography of various sizes from intruders.

THREATS IN PRESENT SECURITY MODULES

Intruders can intrude the security hardware of vehicles for stealing identity or to extract security keys. So,

TPDs are used for saving all secret keys produced during cryptographic approaches in intelligent vehicles, but there are many attacks present with the help of which any unauthorized user can access security keys from these devices. H. Handschuch et.al. described the probing attacks on temper resistance devices [5]. These attacks are not destructive in nature. They simply spy on the execution process and after every cycle, they retrieve one single bit of the security key. These attacks can be applied on public key cryptosystem (secret key encryption schemes) to get their private keys. R. Anderson et.al. define low-cost attacks on tamper resistance devices [6]. These tamper proof devices are not absolute secure anyone who has the semiconductor test equipment can retrieve the security keys stored in these devices or chips by observations and manipulations. This lets us conclude that all cryptographic approaches and protected hardware modules are not enough for the security of data. So, we need some more advanced techniques for security.

STANDARDIZED PARAMETERS FOR ELLIPTICAL CURVE CRYPTOGRAPHY

Elliptical curve cryptography (ECC) is the new form of public key cryptography. It was developed by Neal Koblitz and Victor Miller in 1985[7]. They both searched a replacement of discrete log problem (DLP) as Elliptical curve discrete log problem (ECDLP). ECC is based on the algebraic structure of the elliptical curve (E).

E: y2 = x3 + ax+b

Every value of a and b gives a different elliptical curve and also a, b are the elements of the finite field with Pn elements. Every point (x, y) satisfy the elliptical curve equation and a point at infinity lies on the elliptical curve. The public key is also a point on the elliptical and can be obtained from private key by multiplying it with a generator point ‘P’ on the curve. ‘P’ is also a prime number greater than 3[8]. When elliptical curve cryptography is used for encryption and decryption then some public parameters are shared between various users. These parameters depend on the standardization used in the approach. NIST- approved parameters; ANSI X9.62; SECG and Brain pool are some of the standardizations. In this paper, we will work on SECG. SECG also proposed many different specifications for different key sizes. Here we will use secp112r1, secp128r1 and secp160r1 [9]. Table-1 shows the specifications used in our research with their strength and key sizes. This table also points out the key sizes used in RSA/DSA with same security strength.

Table 1: Different Specifications with their Strength and Key Sizes

Parameters	Strength	Size	Value of P	RSA/DSA (Size)
Secp112r1	56	112	$(2^{128}-1)/76439$	512
Secp128r1	64	128	$2^{128}-2^{97}-1$	704
Secp160r1	80	160	$2^{160}-2^{31}-1$	1024

EXPERIMENTAL SETUP

We present here the series of steps required for undertaking the simulation work.

Reading Keys from Temper Proof/ Resistance Devices

Keys are first to read from the intelligent vehicle. Table-2 shows some private keys produced during cryptographic operations with different specifications of ECC. These keys are first converted into hexadecimal form.

Table 2: ECC’s Private Keys Used in Network for Training

<table>
<tr><th>Specification</th><th>ECC 14 Standard Private Key</th><th>Keys in Hexadecimal Form</th></tr>
<tr><td>Secp112r1</td><td>!DY|$x(-;s^38;&590</td><td>0D8C6CDFCE7D</td></tr>
<tr><td>Secp128r1</td><td>!i7I:$H103Y$VgGRaS@%</td><td>8BB207D74DD856019169</td></tr>
</table>

Secp160r1	31H35IUF-ctDgWc<?=5%,#t{_	DF51F7E4850572D0E059

Changing Keys in Binary Form

In this phase, keys are converted into binary form and reshaped to form matrices.

Training Network

In this phase, private keys in the binary form obtained from the previous phase are taken as input and target values. The network is then trained using feed forward back propagation model. ‘Trainlm’ function is used as a training function. ‘Tansig’ and ‘purelin’ functions are used as the activation function.

Replacing Keys with Network Parameters

After training, the network parameters are saved in the hardware and the alphanumeric keys are deleted from the memory. Figure-1 shows the steps involved in our network model.

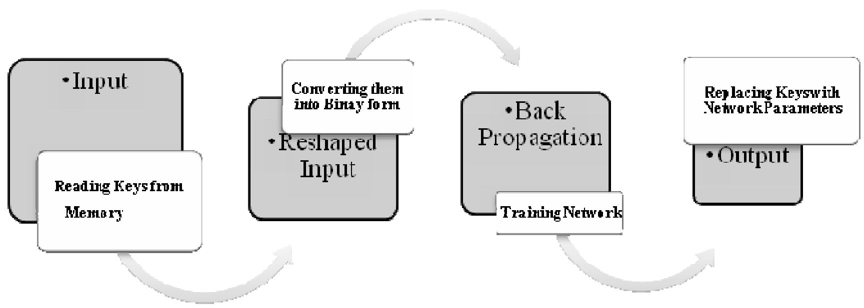

Figure 1: Neural Network Based Security Network

RESULTS AND OBSERVATIONS

Three different specifications with different input and output values are trained using the same number of neurons in input layer, hidden layer, and an output layer. Network parameters are also same in all experiments. Each experiment took different time for training and number of epochs also varies for learning.

Table 3: Epochs and Time Taken by Different Specifications

Specification	Bits in Private Key(in Binary Form)	Epochs	Time
secp112r1	192	4+4+5+5= 18	0.04 sec
secp128r1	320	5+6+6= 17	0.03 sec
secp160r1	384	4+5= 9	0.02 sec

The network, once trained, will not show same training again. Figure-2 shows the training model used in our research. Every time we train the network for same input values the weight values will differ. Table-3 represents the number of epochs and time taken by each specification during training. Specification first i.e. secp112r1 took 18 epochs but we trained the network 4 times to get desired output. Specification second i.e. secp128r1 took 17 epochs but we trained the network 3 times to get desired output. Specification third took 9 epochs in 2 pieces of training.

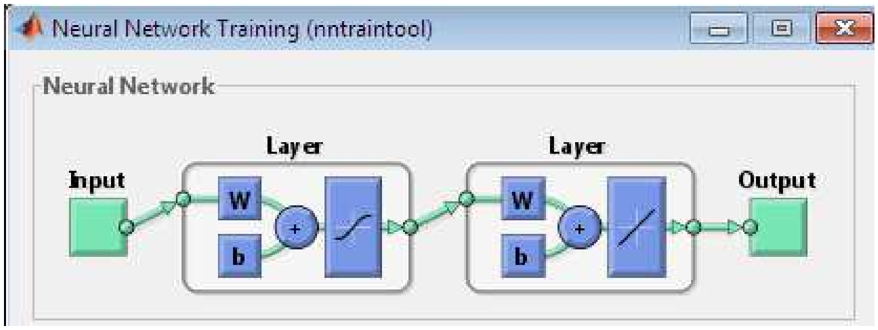

Figure 2: Network Model used for Training Process

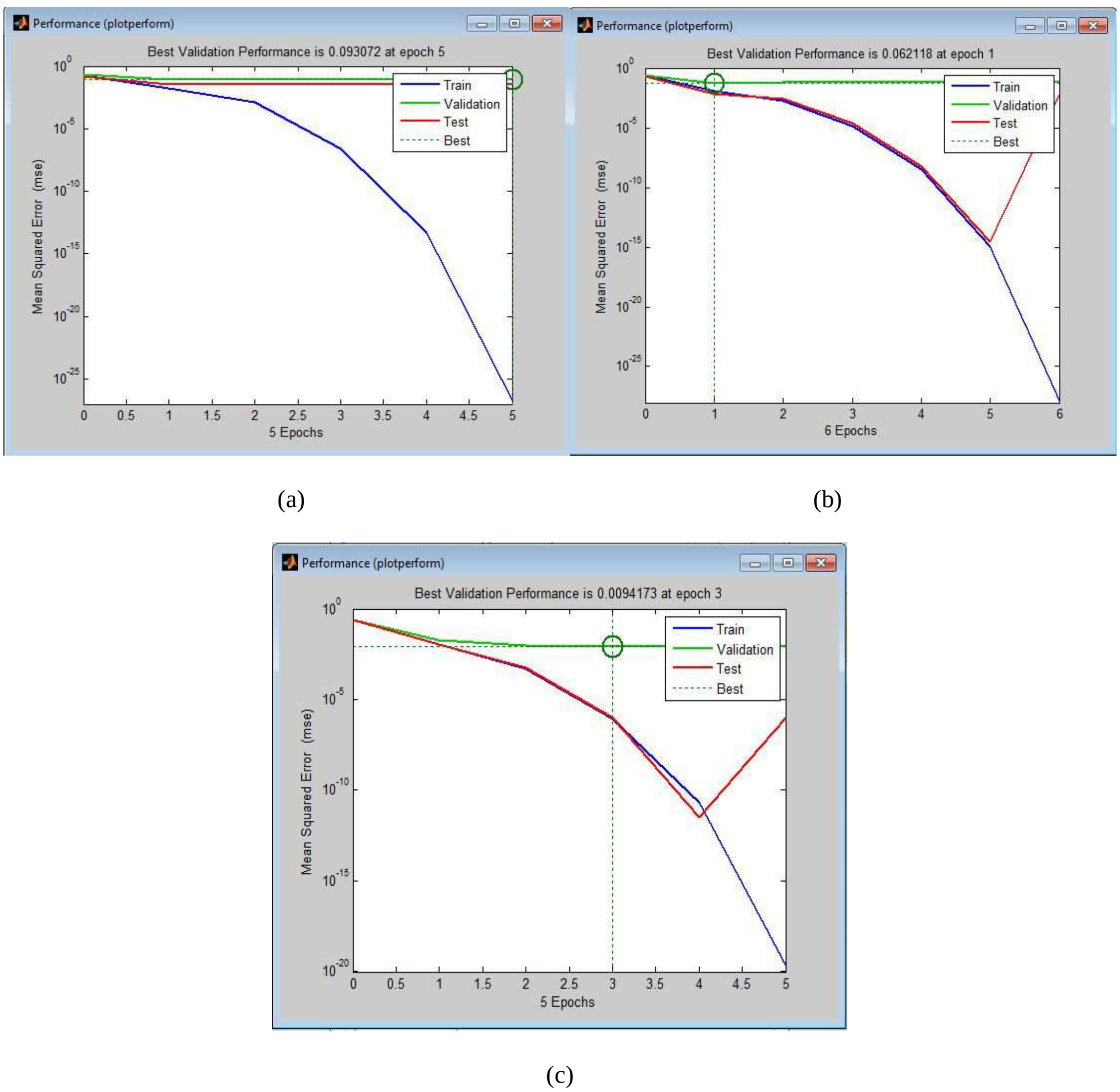

Figure 3: Performance of (a) Training 4 of Secp112r1, (b) Training 3 of Secp128r1 and (c) Training 2 of Secp160r1

Figure 3 (a), (b) and (c) show various performance graphs of training obtained during our experiment. In each graph, variation of mse(mean squared error) w.r.t. the epochs of the network are drawn and also the best validation value is

given at the top of the graph. Here three graphs of last training are given. All three graphs are the result of the best training during the learning process.

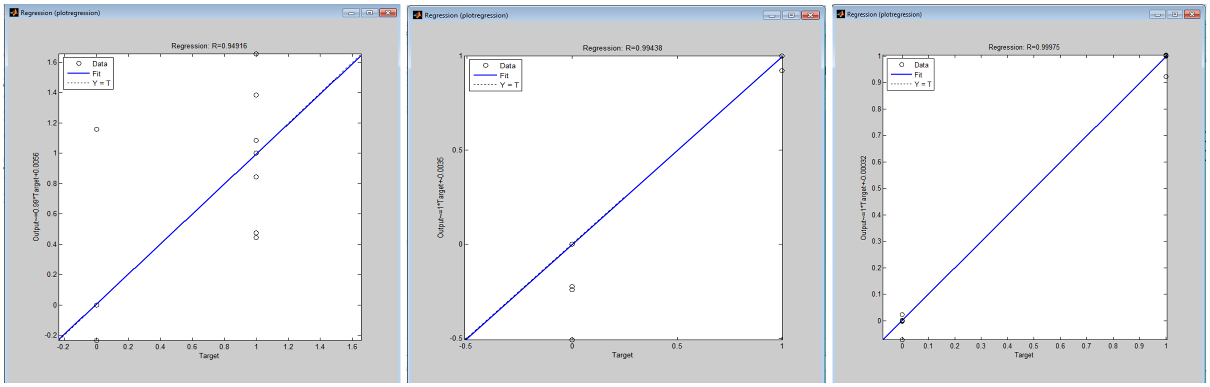

Figure 4: Regression Testing of Three Specifications

Figure 4 (a), (b), (c) show the regression testing done after training processes. In all these Figures, network outputs are compared with the target outputs.

CONCLUSIONS

In this paper, neural network based security mechanism for keys generated during ECC in VANETs is described. Parameters obtained from the training using back propagation are saved in the EEPROM of TPDs in place of alphanumeric keys. Three different keys and specifications (secp112r1, secp128r1 and secp160r1) are used in our research and from the results, we find out that secp160r1, which produce security key of maximum size 160 bytes is the best among three, because, the training time and performance of the network is the best for this size of keys.

REFERENCES

1. *J. B. Evans, W. Wang, and B. J. Ewy, "Wireless networking security: open issues in trust, management, interoperation and measurement," Int. J. Secur. Networks, vol. 1, no. 1/2, p. 84, 2006.*
2. *A. Naveena and K. R. Reddy, "A Review : Elliptical Curve Cryptography in Wireless Ad-hoc Networks," pp. 1786–1789, 2016.*
3. *R. Shaikh and D. Deotale, "A Survey on VANET Security using ECC," vol. 4, no. 6, 2015.*
4. *R. K. Pooja and U. K. N. Kalyane, "VANET BASED SECURE AND EFFICIENT TRANSPORTATION SYSTEM," pp. 2319–2322, 2015.*
5. *H. Handschuh, P. Paillier, and J. Stern, "Probing Attacks on Tamper-Resistant Devices," Igarss 2014, vol. 1717, no. 1, pp. 1–5, 2014.*
6. *R. Anderson and M. Kuhn, "Low cost attacks on tamper resistant devices," Secur. Protoc. V, pp. 125–136, 1999.*
7. *N. Koblitz, "Elliptic curve cryptosystems," Math. Comput., vol. 48, no. 177, pp. 203–203, 1987.*
8. *S. S. Manvi, M. S. Kakkasageri, and D. G. Adiga, "Message Authentication in Vehicular Ad Hoc Networks: ECDSA Based Approach," 2009 Int. Conf. Futur. Comput. Commun., 2009.*
9. *https://crypto.stackexchange.com/questions/1895/standardized-parameters-for-elliptic-curve-cryptography?rq=1*

APPENDICES

Vitae

Ekta Narwal, Assistant Professor, Computer Science Department of Mathematics, Maharshi Dayanand University, RohtakHaryana-124001 email- eku.narwal@gmail.com

Dr Sumeet Gill Assistant Professor, Computer Science Department of Mathematics, Maharishi Dayanand University, Rohtak Haryana 124001. Email- drsumeetgill@gmail.com